Índice

1. Introdução 4

2. Implementação e Arquitetura 5

3. Insegurança no Ar 7

3.1. Ataques 9

3.2. Reduzindo os Riscos 13

4. A Estrada do Futuro 19

5. Conclusão 21

RESUMO

Este white paper apresenta inicialmente as características da tecnologia 802.11b. Esta apresentação inicial da tecnologia serve como base para discutir os aspectos de segurança (ou a falta dela) nas redes sem fio. Conhecer os problemas de segurança torna possível analisar, planejar e implementar uma rede wireless com foco em segurança, tópico importante que deve ser visto com muita atenção.

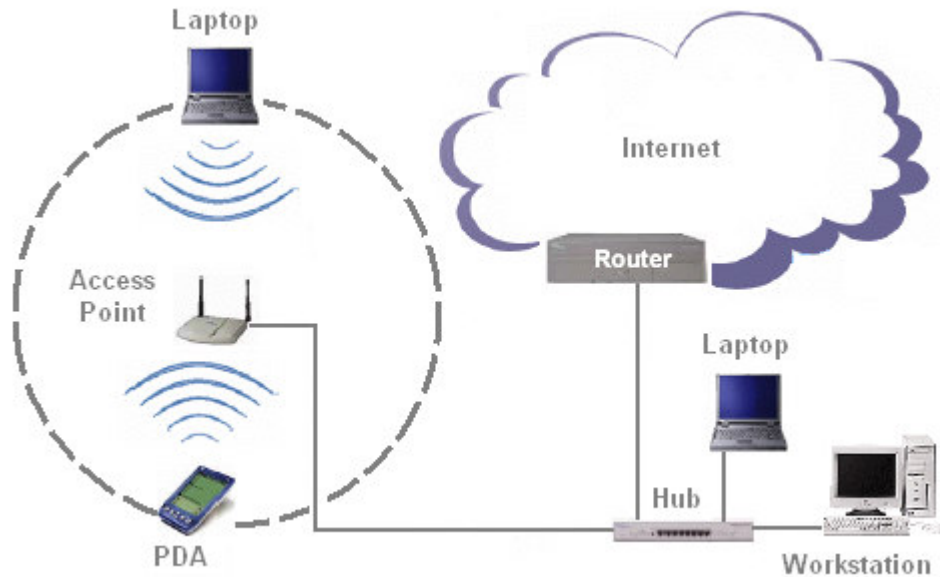
ABSTRACT

This white paper initially presents the 802.11b technology features. This initial presentation of the technology provides us base to discuss the security features (or the absent of it) in wireless networks. Knowing the security issues makes it possible to analyze, plan and implement a wireless network focusing on security, important topic that should be addressed with care.

1. Introdução

Uma rede sem fio é um conjunto de sistemas conectados por tecnologia de rádio através do ar. Pela extrema facilidade de instalação e uso, as redes sem fio estão se difundindo rapidamente por todo o mundo, principalmente na área de saúde e educação. Apesar de os usuários verem apenas o lado positivo, existem questões de segurança importantes relacionadas com as redes wireless. Este paper busca mostrar os problemas das redes sem fios nos 3 âmbitos de segurança (confidencialidade, integridade e disponibilidade) e fornecer recomendações para a redução dos riscos e das vulnerabilidades.

As Wireless Local Area Networks (WLANs) já são populares nos dias de hoje. A pesquisa de mercado do IDC de novembro de 2001 mostra que são fabricados 3 milhões de componentes para WLANs por trimestre. Para o Yankee Group, as WLANs substituirão as redes com fio que temos hoje, por causa de sua flexibilidade e Retorno de Investimento que oferecem, através da redução de custos de implementação e suporte, além do ganho de produtividade. Conforme o relatório publicado em julho deste ano, o número de implementações de redes wireless no Estados Unidos duplicou nos últimos 12 meses e estão atualmente em uso cerca de 1.000.000 de Access Points em 700.000 empresas nos EUA. De acordo com o Gartner Group, em 2005 existirão cerca de 137 milhões de usuários de redes sem fio, a maioria em empresas.

2. Implementação e Arquitetura

O padrão mais usado de redes sem fio no mercado no momento é o 802.11b, apesar de outros padrões já terem aparecido, como o Bluetooth. O padrão IEEE 802.11b é baseado na tecnologia Direct Sequence Spread Spectrum (DSSS) que usa transmissão aberta (broadcast) de rádio e opera na freqüência de 2.4000 a 2.4835 GHz com uma capacidade de transferência de 11 Mbps, em ambientes abertos (~450 metros) ou fechados (~50 metros). Esta taxa pode ser reduzida a 5.5 Mbps ou até menos, dependendo das condições do ambiente no qual as ondas estão se propagando (paredes, interferências, etc). Por ser uma transmissão aberta, qualquer pessoa com um receptor operando na mesma freqüência pode captar as ondas. Assim como em um passeio de carro, conforme nos afastamos da estação de rádio transmissora o sinal começa a ficar cada vez mais fraco até que não possamos mais captá-lo. Conforme formos chegando mais perto da transmissora, o nosso receptor conseguirá mais facilmente captar o sinal até chegarmos no nível de clareza total na recepção.

Tanto o Access Point quanto o laptop e o PDA transmitem e recebem sinais. Este conceito será usado mais adiante para entendermos métodos de ataque e de segurança.

Característica	Descrição
Camada Física	DSSS
Freqüência	2.4 GHz
Método de acesso	CSMA/CA
Taxa de transmissão	1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps
Propagação	50 metros (ambiente fechado) 450 metros (ambiente aberto)
Capacidade	11 Mbps (54 Mbps planejados)
Prós	Grande quantidade de fornecedores, preços cada vez mais baixos
Contras	Segurança fraca, capacidade de tráfego pode vir a sofrer um gargalo

Tabela 2.1.1 – Características da tecnologia 802.11b

Figura 2.1.1 - Exemplo de uma rede 802.11b

WEP

O Wired Equivalency Privacy (WEP) é o método criptográfico usado nas redes wireless 802.11. O WEP opera na camada de enlace de dados (data-link layer) e fornece criptografia entre o cliente e o Access Point. O WEP é baseado no método criptográfico RC4 da RSA, que usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada (secret shared key) de 40 ou 104 bits. O IV é concatenado com a secret shared key para formar uma chave de 64 ou 128 bits que é usada para criptografar os dados. Além disso, o WEP utiliza CRC-32 para calcular o checksum da mensagem, que é incluso no pacote, para garantir a integridade dos dados. O receptor então recalcula o checksum para garantir que a mensagem não foi alterada.

3. Insegurança no Ar

O IEEE 802.11b define dois métodos de autenticação: um usando criptografia e outro não. O método que não usa criptografia se divide em dois: o método aberto e o fechado. No método aberto, Access Points (APs) e clientes enviam beacons e broadcasts, respectivamente, em determinados intervalos de tempo para que um possa saber da existência do outro. Beacons são como convites para que os clientes saibam da existência do AP, contendo informações sobre que canal devem usar para acessa-lo e o Service Set ID (SSID), que é uma seqüência de caracteres (como um nome) que identifica uma rede entre outras que estejam operando na mesma freqüência. O número do canal vai de 1 a 11 (1 a 13 na Europa). A tabela 2.1.2 contém a numeração dos canais:

Canal	Freqüência (GHz)
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

Tabela 2.1.2

O método fechado exige que o cliente responda com o nome correto do SSID para que possa acessar a rede. Ambos os métodos são primitivos e extremamente vulneráveis.

O método criptográfico utiliza chaves compartilhadas para autenticar o cliente no AP. Através de chaves WEP pré-definidas no AP e nos clientes, a autenticação é processada e apenas autentica o cliente no AP. Este método não consegue autenticar o AP para o cliente, fazendo com que o cliente não tenha a garantia de que está se comunicando com um AP autorizado ou não. A figura 2.1.2 mostra o método criptográfico de autenticação.

Figura 2.1.2 – Autenticação do cliente feita com "shared keys"

Outro problema é que, para fazer com que as redes sem fio possam ser colocadas em funcionamento com rapidez, os mecanismos de segurança existentes nos equipamentos costumam vir desabilitados, isso quando existem. Este é o problema principal das redes sem fio: 80% delas não usam nem mesmo os mecanismos básicos de segurança, de acordo com a pesquisas feitas em 2002.

O pouco entendimento sobre arquitetura de redes faz com que o profissional não entenda exatamente como a rede sem fio funciona e como ela se encaixa no ambiente já existente. Uma boa ou má implementação da rede sem fio na corporação poderá fazer a diferença entre riscos gerenciáveis e riscos inaceitáveis.

Por exemplo, não é trivial especificar com exatidão qual é o alcance de rede wireless. De acordo com o paper Wireless Network Security do NIST[1] (National Institute of Standards and Technologies), devido às diferenças entre construções de prédios, freqüências e atenuações e antenas de alta potência, a distância correta para o controle da propagação das ondas pode variar consideravelmente, alcançando quilômetros mesmo que a especificação técnica do equipamento mencione apenas poucas centenas de metros.

Na rede de fios, existe um, ou alguns pontos de acesso à sua rede, como a Internet, por exemplo. Na rede sem fio, qualquer ponto localizado geograficamente em um espaço de ~50 a ~450 metros de distância nas 3 dimensões pode ser usado para acessar a sua rede. Por isso é imprescindível o uso de métodos de detecção de Access Points não autorizados na rede.

A facilidade de acesso é tão grande que há quem diga que implementar uma rede WLAN é o mesmo que "jogar 300 metros de cabeamento de rede pela janela" ou "colocar um hub no estacionamento e permitir que qualquer um se conecte na rede como se estivesse dentro da empresa". A realidade

[1] Acesse www.nist.gov

não é muito diferente desta analogia, e por este motivo é extremamente importante que antes da implementação da rede sem fio, quesitos de segurança sejam analisados.

Durante a conferência hacker Defcon[2] X, ocorrida no início de agosto em Las Vegas, foram detectados mais de 10 novos tipos de ataques, segundo a AirDefense[3]. Uma parte destes ataques foi identificada como sendo novos tipos de Denial of Service. A outra parte, mais preocupante, revelou ataques mais sofisticados que exploram falhas dos protocolos 802.11, o que mostra que os hackers estão se aprofundando em redes wireless 802.11.

3.1. Ataques

WLAN Scanners

Como foi mencionado, qualquer equipamento operando na mesma freqüência pode captar os sinais transmitidos através do ar. Desabilitar o envio de broadcasts no AP não impede que scanners como o NetStumbler[4] (plataforma Windows) detectem a rede enviando pacotes em todos os canais para ver em qual o AP responde. Além de captar informações da rede, alguns scanners como o NetStumbler possuem a capacidade de dizer onde esta localizada a rede através do uso de equipamentos de GPS. Isto se torna muito conveniente caso o hacker decida voltar mais tarde para capturar pacotes ou quebrar a chave WEP. Os adeptos de PocketPC podem procurar WLANs usando o MiniStumbler, uma versão não tão poderosa do NetStumbler que está disponível no mesmo site.

WLAN Sniffers

O Kismet[5] (plataforma Linux) apesar de não suportar ambiente gráfico, além de ser um scanner também funciona como sniffer. Enquanto procura Access Points, os pacotes capturados podem ser armazenados para uma analise posterior, com o uso de um programa que quebre chaves WEP nos pacotes que o Kismet detecta que possui chave WEP fraca. Outros programas do gênero são: Ethereal para Windows e Linux e TcpDump para Linux.

Denial of Service (DoS)

A freqüência 2.4 GHz é compartilhada com outros dispositivos sem fio como, por exemplo, telefones sem fio, dispositivos Bluetooth e equipamentos de monitoração de bebês – também chamados de "babá eletrônica". Por operarem na mesma freqüência, estes equipamentos degradam o sinal fazendo com que a capacidade da rede seja reduzida. Um indivíduo mal intencionado com o equipamento apropriado pode enviar uma grande quantidade de sinais (flood) na mesma freqüência a ponto de fazer com que a rede pare de funcionar.

---

[2] Acesse www.defcon.org
[3] Fonte: www.airdefense.net/eNewsletter/defconx.htm
[4] Acesse www.netstumbler.org
[5] Acesse www.kismetwireless.net

Outro problema relacionado a DoS é o conflito não intencional entre redes próximas, como a de um prédio vizinho. É comum um mesmo fabricante usar o mesmo canal default para todos os equipamentos fabricados. O que pode acontecer nesta situação é, no mínimo, uma rede causar DoS na outra através de interferencia de rádio. Para evitar este problema, deve-se tentar “enxergar” outras redes próximas. Se isto for possível, alterar o número do canal usado para que haja uma diferença de 5 canais entre as duas redes.

Falhas do WEP

Jesse Walker, da Intel, foi um dos primeiros a demonstrar que a chave WEP não é segura independente do seu tamanho[6]. Em uma pesquisa feita por Nikita Borisov, Ian Goldberg e David Wagner da UC Berkeley[7], foi possível quebrar uma chave WEP de 40 bits em 4 horas usando 250 computadores. Também demonstraram que é possível quebrar chaves de 128 bits.

Após a disponibilização de white papers como os citados acima e “Using the Fluhrer, Mantin and Shamir attack to break WEP”, ferramentas para a automatização da quebra de chaves WEP foram criadas para facilitar a tarefa.

Uma destas ferramentas é o AirSnort[8], uma ferramenta escrita para Linux, que necessita de kernel versão 2.2 ou 2.4 e uma placa wireless que use o chipset Prism2. Apesar dos problemas encontrados para conseguir compilar a ferramenta, o AirSnort é uma boa ferramenta para a quebra de chaves WEP. Após colocar a placa wireless em modo promiscuo através de um shell script (dopromisc.sh) que vem junto com a ferramenta, inicia-se o modo de captura de pacotes que serão analisados posteriormente. Durante a captura, o AirSnort mostra o andamento do processo, incluindo o número de pacotes “interessantes”. Assim que for capturado um número suficiente destes pacotes, pode-se iniciar o processo que quebra. De acordo com a documentação da ferramenta, são necessários aproximadamente 1500 pacotes “interessantes” para quebrar uma chave WEP de 128 bits. A criptografia WEP utiliza um vetor de inicialização RC4 para criptografar pacotes com chaves diferentes. Primeiramente isto parece seguro. O problema é que o vetor de inicialização (IV) além de ser incrementado seqüencialmente, possui 24 bits, ou seja, a cada 2^{24} pacotes o IV se repete (este é um pacote interessante). 2^{24} pacotes significam 16.8 milhões de pacotes, que são obtidos em uma rede de 5 Mbps congestionada durante algumas horas.

Outra ferramenta disponível na Internet é o WEPCrack[9]. O WEPCrack é composto por 4 scripts feitos em Perl que são usados para decodificar pacotes, identificar pacotes fracos e quebrar a chave WEP. Para usar o WEPCrack é necessário primeiro capturar o tráfego com um sniffer, pois ao contrário do AirSnort, o WEPCrack não captura pacotes. Um sniffer que pode ser usado é o prismdump[10], que é um add-on para o Ethereal[11], um conhecido capturador de pacotes. Neste ponto o AirSnort leva

[6] Jesse Walker, “Unsafe at any key size; An Analysis of the WEP encapsulation” http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip
[7] Borisov, Nikita; Goldberg, Ian; Wagner, David. “Security of the WEP algorithm”, UC Berkeley. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
[8] Veja mais em www.be-secure.com/airsnort.html
[9] Acesse http://sourceforge.net/projects/wepcrack
[10] Acesse http://developer.axis.com/download/tools/
[11] Acesse http://www.ethereal.com/

vantagem sobre o WEPCrack, já que consegue capturar apenas os pacotes necessários para a quebra de criptografia, enquanto no caso do WEPCrack é necessário capturar todo o tráfego primeiro para que se possa alimentar os scripts Perl, o que consome grande espaço de disco rapidamente.

Também existe um problema já relatado em relação à falha de integridade. O WEP utiliza CRC-32 para calcular o checksum da mensagem que é incluso no pacote. De acordo com um relatório da Universidade de Berkeley, por utilizar um método de CRC linear, é possível alterar a mensagem e recalcular a diferença de checksums entre a mensagem original e a alterada, fazendo com que o receptor não identifique a alteração da mensagem.

Access Points não autorizados

Assim como acontece de um usuário instalar um modem no computador para acessar a Internet, pode haver Access Points não autorizados (e com configuração default ou mal configurados) na rede da empresa. O custo cada vez mais baixo deste tipo de equipamento deve ser uma preocupação para os administradores. Além do uso inadvertido de Access Points pelos funcionários, pode ter sido instalado um AP na rede com o propósito de capturar pacotes para depois descriptografá-los. O invasor pode configurar o AP com um sinal mais forte do que os demais para que ele seja o primeiro AP detectado pelos clientes. Este AP é então utilizado para capturar nomes de usuários, senhas e outras informações.

Roubo de equipamento

Em caso de roubo de equipamento wireless, a rede pode ser acessada sem que os administradores tenham conhecimento. Isto acontece porque o equipamento já está configurado para acessar a rede. Neste caso, pode ser necessário reconfigurar a rede para eliminar esta vulnerabilidade. A política de segurança deve requerer que os usuários notifiquem os administradores da rede em caso de perda ou roubo de laptops ou PDAs e os usuários devem ser educados neste sentido.

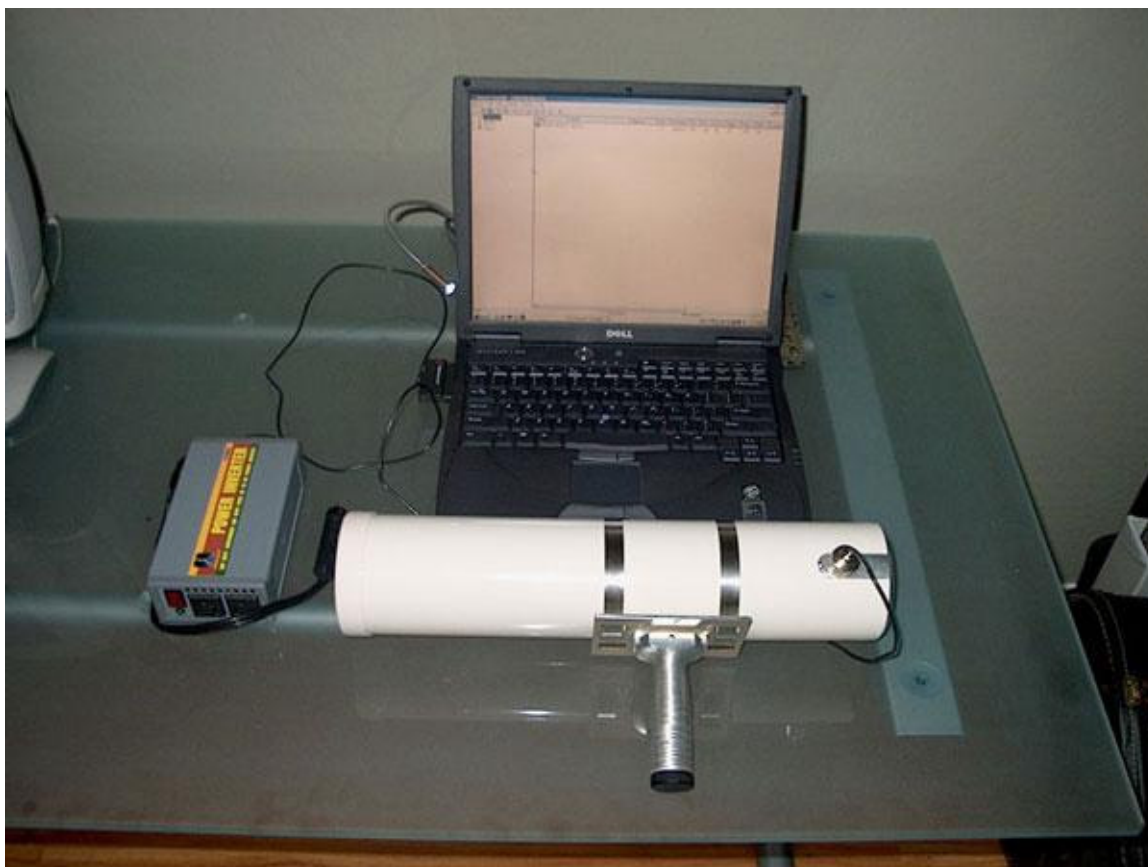
Uso indevido de recursos e perda de rastreabilidade

Indivíduos podem usar redes wireless de terceiros para simplesmente:

a) não pagar acesso à Internet;

b) ter acesso à Internet na rua;

c) invadir outras redes wireless sem que possa ser rastreado, afinal qualquer informação rastreada levará até a rede que foi invadida.

Wardriving / Warchalking[12]

Da técnica “Wardialing” que consistia em discar um determinado grupo de números de elefone para ver qual deles respondia com um modem, originou-se o nome “Wardriving”. A técnica “Wardriving”

[12] Para mais informações acesse www.warchalking.org

consiste em pegar um laptop com equipamento wireless, e sair andando pela cidade em busca de Access Points. Andando de carro a uma velocidade 70 km/h, ainda é possível detectar APs.

A figura 3.1.1 mostra o "Prophet Wardriving Kit" usado na décima Defcon, durante a conferência sobre redes wireless. Com estes equipamentos, que podem ser facilmente adquiridos, é possível detectar redes (APs), capturar tráfego e até mesmo quebrar a criptografia WEP, obtendo acesso não autorizado aos dados transmitidos na WLAN.

Figura 3.1.1[13] – "Prophet Wardriving Kit": A "pistola" desencaixa para facilitar o carregamento.

Com base nesses "passeios", criou-se o hábito de registrar no mapa, no prédio ou na calçada (nos dois últimos com giz), o lugar onde é possível conseguir acesso wireless. Esta prática recebeu o nome "Warchalking" (chalk significa giz), e é originária da língua dos "hobos" (vagabundos, na gíria inglesa) que, durante a grande depressão americana de 1929, buscavam lugares onde pudessem ser acolhidos e com marcas de giz, informavam os companheiros sobre as condições do lugar. Informações sobre os símbolos dos "hobos" estão no endereço www.worldpath.net/~minstrel/hobosign.htm.

[13] Figura do site www.wardriving.info

Em relação à mapas, o site http://mapserver.zhrodague.net oferece um serviço de mapeamento de APs em todo o mundo com o uso de GPS. Usuários que tenham informações da localização de APs no formato do NetStumbler podem fazer upload. Veja a seguir um outro tipo de mapa, feito no Microsoft MapPoint 2002[14] com o auxílio da ferramenta StumbVerter, disponível em http://www.sonar-security.com/, que importa os dados capturados pelo NetStumbler. O sinal vermelho na parte inferior da pirâmide significa WEP habilitado.

Figura 3.1.2[15] – Mapa feito com Access Points detectados na área da Califórnia

3.2. Reduzindo os Riscos

Vamos discutir agora as medidas de segurança que eliminam ou reduzem os riscos e as vulnerabilidades das redes wireless. As medidas podem ser aplicadas separadamente ou em conjunto.

Trocar o SSID

Todos os APs propagam o SSID em broadcast para que os clientes saibam quais redes estão disponíveis para acesso. O SSID não é criptografado pelo WEP. SSIDs default dos fabricantes não

[14] Acesse www.microsoft.com/mappoint
[15] Figura do site www.wardriving.info

devem ser usados por serem de conhecimento público, e serão os primeiros a serem testados pelo invasor. Recomenda-se o uso de um SSID que não seja de fácil dedução.

Desabilitar o envio de pacotes beacon

Alguns APs possuem a opção de desabilitar o envio de beacons periódicos, fazendo com que o dispositivo wireless do cliente só consiga se conectar se estiver utilizando o mesmo SSID no início da conexão. Caso exista, essa opção deve ser ativada para evitar a captura do SSID feita pelos scanners.

Filtrar endereços MAC

Muitos fabricantes fornecem em seus equipamentos a capacidade filtrar endereços MAC criando uma lista de controle de acesso (ACL) que é distribuída entre os APs[16]. A lista fornece ou nega o acesso do equipamento baseado no endereço MAC. Como o endereço MAC trafega sem criptografia pelo ar, não representa um bom mecanismo de defesa. Tudo que o hacker precisa é capturar o tráfego, e falsificar (spoof) o seu próprio endereço MAC para ter acesso à rede. O esforço administrativo necessário para manter uma lista atualizada de endereços MAC (assumindo que uma lista seja usada) dependendo do número de clientes pode não compensar a pouca segurança fornecida por este filtro.

Pode também ser usada a ferramenta arpwatch[17] para restringir o acesso. Esta ferramenta foi inicialmente desenvolvida para redes com fio, mas também pode ser usada em WLANs. Arpwatch funciona monitorando os endereços MAC que entram e saem da rede. Quando surge um endereço desconhecido, é gerado um alerta para os administradores.

Usar WEP

Os especialistas recomendam que não se confie no WEP para criptografia de tráfego por ser inseguro por natureza. Use-o para dificultar o acesso não autorizado na rede. É melhor usar WEP do que não usar nada. Melhor ainda é combina-lo com VPN ou algum método de criptografia de aplicação (como o PGP) e RADIUS.

As chaves criptográficas usadas pelo WEP devem ser trocadas periodicamente, já que um hacker pode quebrá-la em questão de horas. O fato de trocar as chaves implica em reconfiguração de todos os Access Points e clientes wireless, o que pode consumir muito tempo. Atualmente alguns fabricantes fornecem soluções próprias de criptografia que devem ser usadas quando possível. É importante lembrar que soluções proprietárias costumam não funcionar entre fabricantes diferentes.

Os fabricantes de dispositivos wireless estão desenvolvendo métodos de criptografia que evitam os pacotes com “chave fraca”, que são utilizados por ferramentas como AirSnort. Estes métodos são atualizados através de firmware. Para que este método funcione, todos os dispositivos wireless devem ser atualizados.

---

[16] Dave Molta, “WLAN Security On The Rise” www.networkcomputing.com
[17] Ferramenta desenvolvida por Lawrence Berkeley National Laboratory – http://ee.lbl.gov/

Localização centralizada do AP

Recomenda-se instalar os Access Points no centro da área que deve ter acesso à rede. É importante lembrar que os sinais não se propagam apenas horizontalmente, mas sim nas 3 dimensões. Faça de tal maneira que as áreas que necessitam de acesso consigam se comunicar com o Access Point, mas evite que o sinal chegue no estacionamento ou no prédio vizinho. Para conseguir essa informação, o administrador pode fazer um scan ao redor da área desejada.

Segmentando as redes com um Firewall

Por serem inseguras por natureza, redes sem fios apresentam ameaças diferentes das da rede com fios. Um firewall deve ser usado para segmentar as duas redes, permitindo acesso entre as interfaces através de autenticação. Os equipamentos que fazem parte da WLAN junto com o AP devem ser colocados em uma DMZ[18]. Recomenda-se também que o cliente seja protegido através de um firewall pessoal (firecell).

Administração via Telnet, console RS-232, SNMP, HTTP

Alguns cuidados a mais devem ser tomados se o AP suporta administração via telnet, SNMP e HTTP, além do console. Estes cuidados incluem a desativação do método caso não seja usado, alteração das configurações default, uso de senha complexa, entre outros. No caso dos Access Points que usam agentes SNMP, deve alterar o nome da comunidade que costuma ser “public” e possui permissão de leitura ou de leitura e escrita, para um nome de difícil dedução. Caso o único tipo de acesso feito via SNMP seja somente de leitura, deve-se configurar o agente apenas para leitura. Se o SNMP não será utilizado, deve ser desabilitado. No caso da administração via telnet, recomenda-se o uso do SSH[19] (secure shell), que substitui o rlogin e telnet do UNIX, que são conhecidos por serem facilmente explorados. O SSH é visto como uma “VPN simples” e na sua versão atual se integra a soluções de PKI, smart cards, LDAP e AES (Advanced Encryption Standard), que substitui o DES (Data Encryption Standard). O HTTP pode ser substituído pelo SSL[20], que faz criptografia na camada 6 do modelo OSI.

VPN

O uso de VPNs[21] (Virtual Private Networks) é recomendado para dar proteção adicional à criptografia do tráfego. A maioria das VPNs hoje em dia, utiliza o protocolo IPSec, que é independente do método de criptografia do WEP, possibilitando o uso de ambos na rede. O IPSec opera na camada de rede (camada 3) do modelo OSI, criptografando os dados que vem das camadas superiores, como a camada de aplicação e transporte (camadas 7 e 4), por exemplo. O WEP trabalha na camada de enlace de dados (data-link – camada 2). Também é possível habilitar o log de atividades no VPN Gateway, para uma posterior auditoria e interpretação de quais usuários estão se logando

---

[18] De-Militarized Zone – um termo usado na área de redes que descreve um segmento de rede onde usuários externos são permitidos acessar recursos sem ter acesso à rede interna.
[19] Uma versão open source do SSH pode ser encontrada em http://www.openssh.org/
[20] Acesse http://www.openssl.org/
[21] Para uma lista de fabricantes, visite o VPN Consortium ou VPNC em http://www.vpnc.org/. Este site é de uma organização comercial criada por diferentes fabricantes.

na rede. A implementação de VPNs pode se tornar complexa, devido à incompatibilidade entre fabricantes.

Usar RADIUS (autenticação)

O RADIUS (Remote Authentication Dial-in User Service) pode ser usado para centralizar a base de contas usadas para autenticar usuários na WLAN. Além disso, o RADIUS também suporta a autenticação de clientes VPN. Deve-se consultar o manual do Access Point para saber se há suporte a autenticação via RADIUS.

DHCP em WLANs

Se possível, o DHCP deve ser evitado na WLAN. Após o usuário conectar seu laptop ao Access Point, ele precisa de um IP válido para poder se comunicar. O servidor DHCP fornece então automaticamente um endereço IP e outras configurações da rede. Por não saber quais são os dispositivos wireless autorizados na rede, o DHCP automaticamente atribuirá um endereço IP válido ao intruso. A remoção do serviço DHCP na WLAN não impedirá que o hacker consiga trafegar na rede. Esta medida é tomada para dificultar o acesso do hacker, que para descobrir a faixa de endereços IP válidos, pode passar algum tempo capturando e analisando pacotes. Ou ainda pode tentar se conectar fazendo um “brute force” de endereços privados, já que as faixas disponíveis são limitadas. Endereços IPs estáticos devem utilizados sempre que possível.

Simulação de APs

O programa Fake AP da Black Alchemy[22] cria beacons falsos de 802.11b com ESSID, BSSID (MAC) aleatórios em vários canais, fazendo com que ferramentas de wardriving como o Netstumbler e Kismet identifiquem milhares de APs. Access Points falsos podem ser usados como parte de uma solução de segurança ou de um sistema de honeypot. Esta ferramenta roda em Linux e necessita de uma placa wireless com chipset Prism2/2.5/3 além dos drivers HostAP[23]. A ferramenta também suporta WEP e a opção variar a capacidade de propagação.

Compartilhamento de Arquivos

Se não for necessário compartilhar pastas e impressoras na rede sem fio, o compartilhamento de arquivos (File Sharing) deve ser desabilitado. Esta é uma medida de segurança adicional.

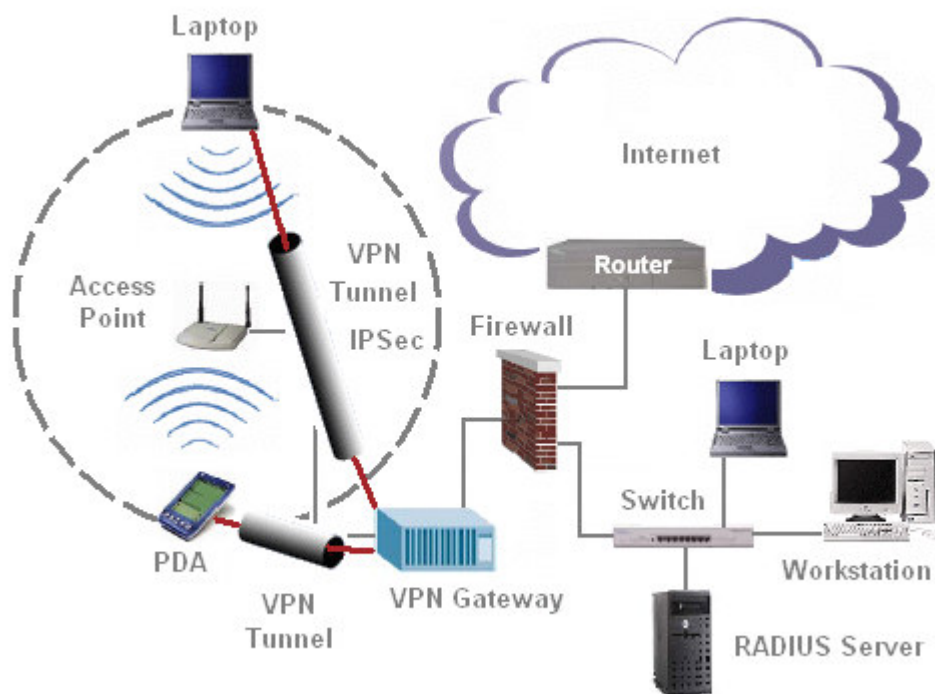
Access Points não autorizados

A melhor maneira de identificar APs não autorizados na rede é pegar um laptop com uma placa wireless e fazer uma “busca aérea” usando scanners. Esta busca deve ser feita periodicamente.

Problemas do TCP/IP já conhecidos

[22] http://www.blackalchemy.to/Projects/fakeap/fake-ap.html
[23] http://hostap.epitest.fi/

Além de todos os problemas já mencionados, ficamos sujeitos aos problemas de segurança inerentes do TCP/IP que já são bem conhecidos, como flooding, spoofing, sniffing, man-in-the-middle, poisoning, entre outros.

Segurança Física

O conceito de segurança física deve ser revisto, afinal estes conceitos simplesmente não se aplicam às redes wireless. Não é necessário entrar na empresa para ter acesso à rede. A partir do estacionamento ao lado é possível se conectar, ou até mesmo a muito metros de distância, dependendo das condições do ambiente e da força do sinal. Manter um guarda vigiando os visitantes o tempo todo pode não trazer resultados, afinal, é possível capturar dados usando um PocketPC ou um iPaq no bolso da jaqueta. Com a ajuda do GPS, o hacker pode voltar mais tarde aos lugares mapeados e a partir de um lugar público, se conectar à rede.

Já nos foi relatado um caso em que a rede wireless foi usada porque não era possível alterar a construção do prédio, em virtude de o mesmo ser tombado pelo patrimônio histórico. Como havia a preocupação com segurança, a medida escolhida foi selar o ambiente com placa de chumbo, evitando assim que o sinal do AP fosse detectado fora do ambiente.

De qualquer forma, esforços podem ser empregados para reduzir este risco. Se o sinal puder ser detectado fora do prédio, considere o uso de câmeras ou guardas no local para tentar detectar ataques “wardriving” ou “warwalking”.

Além das recomendações descritas acima, deve-se considerar o uso de IDSs, principalmente no momento de implementação, registrando todas as atividades. O AP deve ser desligado quando não estiver sendo usado, e um inventário completo dos APs e dispositivos wireless deve ser feito.

Figura 3.2.1 – Exemplo de uma rede 802.11b com alguns mecanismos de segurança

4. A Estrada do Futuro

TKIP

O relatório 802.11i especifica o uso do Temporal Key Integrity Protocol (TKIP), para eliminar as falhas já conhecidas do WEP. O TKIP[24] é uma tentativa do IEEE de dar mais segurança as redes wireless enquanto mantém a compatibilidade com os equipamentos já fabricados.

AES

O uso de AES em substituição ao uso do WEP está sendo considerado pelo 802.11i, já que o TKIP é uma solução imediata e o WEP precisa ser substituído por completo. O AES suporta chaves de até 256 bits e utiliza “block ciphers” maiores.

802.1x

A força-tarefa de segurança 802.11i define o uso de Extensible Authentication Protocol (EAP) over LANs (EAPOL) para aumentar o nível de segurança no 802.1x. O EAPOL será usado para autenticar clientes quando eles se conectarem a rede[25]. Deste modo, hackers não conseguiriam acessar a rede apenas identificando o canal e o SSID da rede utilizando um IP válido para capturar pacotes de modo passivo. O 802.1x foi padronizado recentemente pelo IEEE e é suportado apelos maiores fabricantes de software e hardware, como Microsoft, que já o implementou no Windows XP, e Cisco, que já implementou o 802.1x nos seu equipamentos wireless. O padrão 802.1x suporta além do EAP, o RADIUS como método de autenticação.

Capacidade do meio aéreo

Os avanços na rede sem fio ocorrem muito lentamente, se comparados aos avanços da rede de fios. O próximo passo é chegar a 22 Mbps enquanto redes com fios falam a 1 Gbps. Por enquanto, com um número limitado de usuários, 11 Mbps está sendo suficiente. Mas com um número maior de usuários, conforme as previsões de crescimento da rede, pode haver um gargalo no fluxo. Já existem equipamentos no mercado que suportam 22 Mbps. Alguns suportam ambos os padrões.

Autenticação

Soluções de autenticação incluem o uso de logins com senha, biométrica, smart cards e PKI (Public Key Infrastructure). Quando a autenticação for baseada em nomes de usuário com senha, deve-se usar um número mínimo de caracteres, um tempo máximo de expiração da senha, entre outras configurações. Em futuro próximo poderá ser adotada uma solução de PKI onde o usuário precisa primeiro destravar o seu certificado digital X.509 através de senha para depois poder usar este certificado para acessar a rede. Pode-se considerar o uso de PKI com smart cards caso sejam necessários níveis adicionais de segurança.

---

[24] Jesse Walker, “802.11 Security Series – Part II: The Temporal Key Integrity Protocol (TKIP)” em http://cedar.intel.com/media/pdf/security/80211_part2.pdf
[25] Paul Goransson, “802.1x provides user authentication”, www.nwfusion.com/news/tech/2002/0325tech.html

Avanço na tecnologia sem fio

No princípio, telefones celulares e PDAs possuiam poucas funcionalidades em função do seu tamanho e requerimentos de energia. No entanto, com os avanços constantes da tecnologia, estes aparelhos estão se tornando cada vez mais leves, menos exigentes em relação à energia, menores e mais poderosos. Para se ter uma idéia deste avanço, a próxima geração de telefones celulares chega ao mercado incorporando funçoes de PDA, infravermelho (IR), Internet sem fio e GPS.

Tecnologias baseadas no GSM, como General Packet Radio Service (GPRS), Enhanced Data GSM Enviroment (EDGE) e Universal Mobile Telecommunications Services (UMTS) contribuirão para o aumento da taxa de transmissão e capacidade de trabalho em rede e devem trazer novas vulnerabilidades e riscos que precisam ser identificados.

5. Conclusão

Do modo como os jornais e a Internet tratam a nova tecnologia podemos perceber que as redes sem fios já foram aceitas pelos usuários. No entanto, é vital que medidas de segurança sejam postas em prática. Apesar de parecer um desafio prover segurança para equipamentos sem fio, profissionais de Segurança da Informação podem reutilizar muitas das medidas usadas nas redes com fios, assim como foi na época do laptop com modem para acesso discado à empresa.

Não devem ser usadas as configurações default nos equipamentos wireless. Será como um convite para hackers entrarem na rede. Deve-se considerar o uso de mecanismos de alta segurança como controle de acesso, criptografia ponto-a-ponto, EAP e RADIUS e VPNs, especialmente em ambientes corporativos. WEP por si só não deve ser considerado como uma solução de segurança.

A política de segurança deve definir com clareza as restrições sobre a comunicação em WLANs (quais equipamentos são permitidos, que tipo de dados podem ser transferidos na rede e se é obrigatório o uso de métodos de criptografia e autenticação, etc) e o uso indevido de Access Points. Os usuários devem ser alertados sobre os perigos da rede sem fio e a auditoria deve estar habilitada e os registros sendo verificados.

Em conjunto com as medidas de segurança citadas neste documento, outras devem ser consideradas para garantir a segurança da rede sem fio e também da rede com fio já existente no ambiente. Segurança é um trabalho dinâmico, que deve fazer parte do dia-a-dia.

A evolução veloz da tecnologia introduz novas vulnerabilidades. Por este motivo, recomenda-se que seja feita uma análise periódica dos riscos da infra-estrutura de TI, sobretudo das que já disponibilizam as facilidades da comunicação sem fio para seus usuários.